IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No.: 3040
Mark J. **STEFIK,** *et al.*	)	Group Art Unit: 3628
Serial No. 09/777,845	)	Examiner: Frantzy Poinvil
Filed: February 7, 2001	)	
For: **SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS USING DIGITAL TICKETS**	)	

United States Patent and Trademark Office
Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

The following Appeal Brief is submitted in support of the appeal proceedings instituted by a Notice of Appeal filed July 26, 2006, in response to the final Office Action mailed January 26, 2006, in connection with the above-captioned patent application.

TABLE OF CONTENTS

Page No.

I. REAL PARTY IN INTEREST

ContentGuard Holdings, Inc. is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are presently no appeals or interferences known to the Appellants, the Appellants' representative, or the assignee, which will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 15-47 are currently pending in the application. This Appeal is taken from the rejection of claims 15-47, as submitted in the Claims Appendix herewith.

IV. STATUS OF AMENDMENTS

No amendment has been filed or submitted subsequent to the Final Rejection mailed on January 26, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is generally directed to a system for distribution and usage rights enforcement of digitally encoded works.

Accordingly, independent claim 15 of the present application recites a digital right management system, including a secure component, and an interface between the secure component and a software application. The secure component processes requests coming from the software application through the interface. The secure component validates signatures of one or more certificate documents to verify that the software application is compatible with the secure component. In the case of verification of compatibility, the secure component allows operation of the software application. In the case of incompatibility, the secure component refuses to allow operation of the software application through the interface. Independent claim 15 is supported at least by ¶¶ [0086]-[0091] of the Specification, as published.

Dependent claims 16-47 describe additional features of the system of independent claim 15, including, for example, features relating to secure component verification of software applications, self protecting documents, and encryption. Dependent claims 16-47 are supported at least by ¶¶ [0061], [0083], [0086]-[0091], and [0423]-[0435] of the Specification, as published.

As such, the claims of the present invention recite an advantageous system for distribution and usage rights enforcement of digitally encoded works by employing a secure component that validates signatures of one or more certificate documents to verify that a software application is compatible with the secure component.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellants respectfully request the Board to reverse (i) the rejection of claims 15-16, 21-45, and 47 under 35 U.S.C. §102, as being anticipated by *Wyman* (USP 5,204,897), and (ii) the rejection of claims 17-20, and 46 under 35 U.S.C. §103, as being obvious over *Wyman*.

VII. ARGUMENTS

Rejection Under 35 U.S.C. § 102

If all claimed elements/steps are disclosed, expressly or inherently, in a single prior art reference, that reference is said to "anticipate" the claimed invention, thereby invalidating the claim(s) under 35 U.S.C. §102. *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

For a novelty rejection, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). *M.P.E.P.* §2131. Appellants respectfully submit that the Examiner has failed to set forth a *prima facie* case of anticipation, since *Wyman* does not expressly or inherently disclose each and every element of claims 15-16, 21-45, and 47.

1. Claims 15-16, 21-22, 24-27, and 30-45, and 47 are not anticipated by *Wyman*

Claims 15-16, 21-22, 24-27, and 30-45, and 47 have been rejected under 35 U.S.C. §102 as anticipated by *Wyman*. This rejection is respectfully traversed and reversal of the Examiner's position with respect thereto is earnestly solicited in that *Wyman* neither discloses nor suggests that which is presently set forth by Appellants' claimed invention. For example, independent claim 15 (emphasis added) recites:

> A digital right management system, comprising:
> a secure component;
> an interface between said secure component and a software application;
> said secure component processes requests coming from said software application through said interface;
> **said secure component validates signatures of one or more certificate documents to verify that said software application is compatible with said secure component**;
> **in the case of verification of compatibility, said secure component allows operation of said software application**; and
> **in the case of incompatibility, said secure component refuses to allow operation of said software application through said interface**.

Thus, independent 15 is directed to the novel features of employing a secure component that validates signatures of one or more certificate documents to verify that a software application is compatible with the secure component.

By contrast, as admitted by the Examiner at page 2 of the non-final Office Action mailed May 9, 2006, *Wyman* discloses a "secure container or environment [that] validates signatures of one or more documents **to verify that one the one or more documents are compatible with the secure container**." However, *Wyman* fails to disclose, teach, or suggest the novel feature of a secure component that validates signatures of one or more certificate documents **to verify that a software application is compatible with the secure component**.

The final Office Action mailed January 26, 2006 states at page 3 that "the Examiner does not find any significant differences, but merely a change in label or in the wordings between the prior claims and the instantly amended claims." Appellants, however, note that the previous claims recited "said secure container **validates signatures of** one or more **documents to verify** that said one or more **documents are compatible** with said secure container" while the present claims recite "said secure component

validates signatures of one or more **certificate documents to verify** that said **software application is compatible** with said secure component," and which is not a mere change of labeling.

However, the final Office Action merely repeats its previous rejection and thus fails to address how *Wyman* discloses, teaches, or suggests a secure component that validates signatures of one or more certificate documents to verify that a software application is compatible with the secure component, as recited in independent claim 15. Specifically, the Examiner relies on *Wyman*, as follows (see p. 2, of the final Office Action):

> The secure container or environment validates signatures of one or more documents to verify that the one or more documents are compatible with the secure container (column 11, line 31 to column 12, line 59);

However, the portions of *Wyman* cited in the final Office Action do not support the rejection of independent 15. Specifically, column 11, line 31 to column 12, line 59 of *Wyman* states:

To implement these operations, the license management program **11** or **14** contains several functions, including a client interface **31**, a database interface **32**, a management interface **33**, and an interserver interface **34** for communicating with the delegatees **13** (if any). The client interface **31**, as described below, handles the requests received from the user nodes **16**, and returns resulting from these requests. The database interface **32** handles the storing and retrieval of license information in the database **23**, and logging license usage activity to log **24**, and retrieval of this data. The management interface **33** handles the tasks of receiving the product use authorizations from the issuer **25** and maintaining the database **23** via the database interface **32**. The interserver interface **34** handles the task of communicating with the delegatee servers **13**, including transmitting the assigned parts of the product use authorizations, or communicating with other license servers that may be separately executing the license management function; for example, calls for validating calling cards may be made to another such server. If there are no delegatees or no other license servers, then of course the interserver interface **34** has no function, and is idle.

The license document or "product use authorization" forming the basis for the license management activity of the program **11** on the server **10** may be illustrated as a data structure containing the information set forth in FIG. **2**; in actual practice the product use authorization is preferably a more abstract data arrangement, not in such a rigidly structured format as illustrated. For example, the product use authorization as well as similar documents stored in the database **23**, or passed between components of the system of FIG. **1**, may be of the so-called tag-length-value data format, where the data structure begins with an identifying tag (e.g., PUA or product use authorization) followed by a field giving the length, followed by the value itself (the content). One type of data treatment using this tag-length-value format is an international standard referred to as ASN.1 or Abstract Syntax Notation,. In any event, the document **35** illustrated in FIG. **2** is merely for discussing the various items of data, rather than representing the way the information is stored. Some of the fields shown here exist at some times and not others, and some are optional; the product use authorization may also include additional fields not shown or discussed here. Also it should be noted that copies of parts of this type of document are made for the delegatees, so this representation of FIG. **2** is a composite of several documents used in the system of FIG. **1**. The document **35** includes fields **36** identifying the software product by product name, producer, version numbers, release date, etc. The issuer **25** is identified in field **37**, and the licensee (usually the owner of the license server **10**) identified in field **38**. The essential terms of the license grant are then defined in fields **40**–**46**. The start date and end date are specified in fields **40**; these store the exact time (date, hour, minute, second, etc.) when the license becomes valid and when it ends, so licenses may be granted to start at some future time and to end at a particular time. Note that the previous practice has been to specify only the ending date, rather than also a start date as employed here. Each of the nodes, including issuer **25**, servers **10** and **13**, and user nodes **16**, maintain a time value by a local clock referenced to a standard, so inherent in the license management facility is the maintaining of a time standard to compare with the start and end date information in the fields **40**. The units granted are specified in field **41**; the units are an arbitrary quantitative measure of program usage. In a delegatee server **13**, the units field **41** will have some subset of the units field in the original product use authorization. As units are granted to users **16** or delegated, the remaining units available for grant are indicated in a subfield **42** in the copy of the document used by the server. The management policy occupies fields **43**–**46**, and includes style, context, duration and LURDM (license use requirements determination method), as will be explained. The style field **43** specifies whether the licensed units are controlled by an "allocative" style or "consumptive" style, or some other "private" algorithm, where styles are ways used to account for the consumption or allocation of the units. The context field **44** specifies the location and environment in which product use or license management occurs, i.e., a CPU or an individual user or a network, etc. Duration field **45** indicates whether the license granted to a user is by assignment, by transaction, or immediate. The LURDM field **46** indicates the license use requirements determination method, in some cases using a license use requirements table (LURT) seen as field **47**, as will be described.

Additional fields **48**–**54** in the product use authorization **35** of FIG. **2** define features such as delegation authorization, calling authorization, overdraft authorization, combination authorization, token, signature, checksum, etc. These will be described in the following paragraphs.

Accordingly, as noted above, *Wyman* is directed to (1) a system a license management program 11 or 14, including a client interface 31, a database interface 32, a management interface 33, and an interserver interface 34 for communicating with the

delegatees 13 (if any), (2) a license document 35 or "product use authorization" forming the basis for the license management activity of the program 11 on the server 10, and (3) additional fields 48-54 in the product use authorization 35 that define features such as delegation authorization, calling authorization, overdraft authorization, combination authorization, token, signature, checksum, etc. However, the cited portions of *Wyman* fail to disclose, teach or suggest a secure component **that validates signatures of** one or more **certificate documents to verify** that a **software application is compatible** with the secure component.

The remaining portions of *Wyman* are similarly deficient. Thus, *Wyman* fails to disclose, teach, or suggest the novel features of employing a secure component that validates signatures of one or more certificate documents to verify that a software application is compatible with the secure component, as recited in independent claim 15. Therefore, Appellants respectfully request reversal of the final rejection of this claim. The dependent claims 16-47 are allowable on their own merits and for at least the reasons set forth above with respect to independent claim 15.

2. Claims 23, and 28 are not anticipated by *Wyman*

Claims 23, and 28 have been rejected under 35 U.S.C. §102 as anticipated by *Wyman*. This rejection is respectfully traversed and reversal of the Examiner's position with respect thereto is earnestly solicited in that *Wyman* neither discloses nor suggests that which is presently set forth by Appellants' claimed invention.

According to the present invention, dependent claim 23 recites:

> A digital right management system according to claim 15, further comprising one or more self-protecting documents.

Dependent claim 28 recites:

> A digital right management system according to claim 23, wherein said secure component detects whether any of said one or more self-protecting documents is tampered with.

As described above, features of the present invention include a secure component that detects whether a self-protecting document is tampered with.

The Examiner has failed to specifically address where any of these features are disclosed by *Wyman,* but rather makes an omnibus rejection of these features citing to FIGs. 1, 6, and 7 of *Wyman* (see final Office Action, p. 3, lines 3-5). However, FIGs. 1, 6, and 7 of *Wyman* are directed to a distributed computer system to implement license management operations (FIG. 1), a logic flow chart of a program executed by a license server in the system of FIG. 1 (FIG. 6), and a diagram of the calls and returns made in an example of use of calling cards in the system of FIG. 1 (FIG. 7). Specifically, the cited portions of *Wyman* are silent with respect to (emphasis added) **a secure component that detects whether a self-protecting document is tampered with**.

Accordingly, *Wyman* does not disclose the invention recited in dependent claims 23 and 28. Therefore, Appellants respectfully request reversal of the final rejection of these claims.

3. Claim 29 is not anticipated by *Wyman*

Claim 29 has been rejected under 35 U.S.C. §102 as anticipated by *Wyman.* This rejection is respectfully traversed and reversal of the Examiner's position with respect thereto is earnestly solicited in that *Wyman* neither discloses nor suggests that which is presently set forth by Appellants' claimed invention.

According to the present invention, dependent claim 29 recites:

> A digital right management system according to claim 15, further comprising an encryption engine.

As described above, features of the present invention include an encryption engine.

The Examiner once again has failed to specifically address where any of these features are disclosed by *Wyman,* but rather makes an omnibus rejection of these features citing to FIGs. 1, 6, and 7 of *Wyman* (see final Office Action, p. 3, lines 3-5). However, as noted above, FIGs. 1, 6, and 7 of *Wyman* are directed to a distributed computer system to implement license management operations (FIG. 1), a logic flow chart of a program executed by a license server in the system of FIG. 1 (FIG. 6), and a diagram of the calls and returns made in an example of use of calling cards in the system of FIG. 1 (FIG. 7).

Specifically, the cited portions of *Wyman* are silent with respect to (emphasis added) **an encryption engine**.

Accordingly, *Wyman* does not disclose the invention recited in dependent claim 29. Therefore, Appellants respectfully request reversal of the final rejection of these claims.

Rejection Under 35 U.S.C. § 103

A patent may not be obtained if the subject matter sought to be patented would be obvious to a person having ordinary skill in the art to which the subject matter pertains. 35 U.S.C. § 103. A determination of obviousness is a legal conclusion based on underlying findings of fact. *Velander v. Garner,* 348 F.3d 1359, 1363 (Fed. Cir. 2003). The Supreme Court in *Graham v. John Deere*, 383 U.S. 1 at 18, 148 USPQ 459 at 167 (1996), set forth the basic test for patentability under 35 U.S.C. §103:

> Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or non-obviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unresolved need, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter to be patented.

Moreover, in *In re Ehrreich* and *Avery*, 200 USPQ 504, 509-510 (CCPA 1979), the Court of Customs and Patent Appeals further clarified the basic test set forth in *Graham v. John Deere*:

> We must not here consider a reference in a vacuum, but against the background of the other references of record which may disprove theories and speculations in the reference or reveal previously undiscovered or unappreciated problems. The question in a §103 case is what the references would collectively suggest to one of ordinary skill in the art. *In re Simon*, 461 F.2d 1387, 174 USPQ 114 (CCPA 1972). It is only by proceeding in this manner that we may fairly determine the scope and content of the prior art according to the mandate of *Graham v. John Deere*, 383 US 1, 17, 148 USPQ 459, 467 (1966)(Emphasis in original.)

Thus, "[t]he mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination," *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Further,

analyzing the claimed invention as a whole in view of the prior art as a whole, one indicium of non-obviousness is a "teaching away" from the claimed invention by the prior art at the time the invention was made. *See U.S. v. Adams*, 148 USPQ 479 (1966). Essentially, teaching away from a claimed invention is a per se demonstration of lack of *prima facie* obviousness.

Where the prior art provides "only general guidance and is not specific as to the particular form of the invention or how to achieve it, [such a suggestion] may make an approach 'obvious to try,' but it does not make the invention obvious." *Ex parte Obukowicz*, 27 USPQ2d, 1063, 1065 (U.S. Patent and Trademark Office Board of Appeals and Interferences, 1992) and *In re O'Farrell*, 7 USPQ2d 1673, 1681 (Fed. Cir. 1988).

Factors including unexpected results, new features, solution of a different problem, novel properties are all considerations in the determination of obviousness. These secondary considerations (objective evidence of non-obviousness), as outlined in *Graham v. John Deere*, must be evaluated before reaching an ultimate decision under 35 U.S.C. §103. Accordingly, the recognition and solution of a problem is considered indicia of non-obviousness. For example, as the Court of Appeals stated in *In re Sponnable*, "[A] patentable invention may lie in the discovery of a source of a problem even though the remedy may be obvious once the source of the problem is identified. This is *part* of the 'subject matter as a whole' which should always be considered in determining the obviousness of an invention under 35 U.S.C. §103." Donald S. Chisum, *Chisum on Patents* § 5.04[7][c][ii], at 5-506 (Rel. 51, 1994) (quoting In re Sponnable 405 F.2d at 578, 585-86, 160 USPQ 237, 243-244 (CCPA 1969)(emphasis in original).

It should be noted that three criteria must be met to establish a *prima facie* case of obviousness. *M.P.E.P. §2143.* First, there must be some teaching, suggestion or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Second, there must be a reasonable expectation of success. *In re Rhinehart*, 531 F.2d 1048, 189 USPQ 143 (CCPA 1976). Last, the prior art must teach or suggest all the claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Appellants respectfully submit that the Examiner has failed to set forth a *prima facie* case of obviousness, since *Wyman* does not teach or suggest each and every element of claims 17-20, and 46.

1. Claims 17-20, and 46 are not obvious over *Wyman*

Claims 17-20, and 46 have been rejected under 35 U.S.C. §103 as obvious over *Wyman*. This rejection is respectfully traversed and reversal of the Examiner's position with respect thereto is earnestly solicited in that *Wyman* neither teaches nor suggests that which is presently set forth by Appellants' claimed invention.

As described above, claims 17-20, and 46 include the novel features of the present invention of employing a secure component that validates signatures of one or more certificate documents to verify that a software application is compatible with the secure component. However, *Wyman,* as noted above, is deficient with respect to the noted features.

Accordingly, *Wyman* does not disclose the invention recited in dependent claims 17-20, and 46. Therefore, Appellants respectfully request reversal of the final rejection of these claims.

Moreover, the inventions recited in dependent claims 17-20, and 46 recognize and solve problems with conventional Digital Rights Management (DRM) systems, such as that of *Wyman*, for example, as described in Applicants' Specification, as published (emphasis added), as follows:

> [0007] **A system for ensuring that licenses are in place for using licensed products is described in PCT Publication WO 93/01550 to Griswold** entitled "License Management System and Method." The licensed product may be any electronically published work but is most effective for use with works that are used for extended periods of time such as software programs. Griswold requires that the licensed product contain software to invoke a license check monitor at predetermined time intervals. The license check monitor generates request datagrams which identify the licensee. The request datagrams are sent to a license control system over an appropriate communication facility. The license control system then checks the datagram to determine if the datagram is from a valid licensee. The license control system then sends a reply datagram to the license check monitor indicating denial or approval of usage. The license control system will deny usage in the event that request datagrams go unanswered after a predetermined period of time

> (which may indicate an unauthorized attempt to use the licensed product). **In this system, usage is managed at a central location by the response datagrams. So for example if license fees have not been paid, access to the licensed product is terminated**.
>
> [0008] It is argued by Griswold that the described system is advantageous because it can be implemented entirely in software. However, **the system described by Griswold has limitations. An important limitation is that during the use of the licensed product, the user must always be coupled to an appropriate communication facility in order to send and receive datagrams. This creates a dependency on the communication facility. So if the communication facility is not available, the licensed product cannot be used. Moreover, some party must absorb the cost of communicating with the license server**.

By contrast, *Wyman* is no better than Appellants' Background Art and thus fails to recognize or address the noted problems with conventional Digital Rights Management (DRM) systems. Accordingly, dependent claims 17-20, and 46 are patently distinguishable over *Wyman*.

VIII. CONCLUSION

Since the Examiner's final rejections under 35 U.S.C. §§ 102 and 103 are inappropriate for the reasons set forth above, Appellants respectfully request the Board to reverse each ground of rejection.

Respectfully submitted,

NIXON PEABODY, LLP

/Carlos R. Villamar, Reg. # 43,224/
Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080

IX. CLAIMS APPENDIX

The following is a complete listing of claims pending on appeal in this application.

1-14. (Cancelled)

15. A digital right management system, comprising:

a secure component;

an interface between said secure component and a software application;

said secure component processes requests coming from said software application through said interface;

said secure component validates signatures of one or more certificate documents to verify that said software application is compatible with said secure component;

in the case of verification of compatibility, said secure component allows operation of said software application; and

in the case of incompatibility, said secure component refuses to allow operation of said software application through said interface.

16. A digital right management system according to claim 15, wherein said software application comprises a rendering engine.

17. A digital right management system according to claim 16, wherein said rendering engine is connected to a printer.

18. A digital right management system according to claim 16, wherein said rendering engine is connected to a computer monitor.

19. A digital right management system according to claim 16, wherein said rendering engine is connected to a handheld device.

20. A digital right management system according to claim 16, wherein said rendering engine is connected to a wireless device.

21. A digital right management system according to claim 16, wherein said rendering engine is connected to a device with one or more optical communication ports.

22. A digital right management system according to claim 15, wherein said secure component performs rights management.

23. A digital right management system according to claim 15, further comprising one or more self-protecting documents.

24. A digital right management system according to claim 15, further comprising one or more structured storages.

25. A digital right management system according to claim 15, further comprising one or more structured file systems.

26. A digital right management system according to claim 15, further comprising information specifying content types.

27. A digital right management system according to claim 15, further comprising information specifying licenses.

28. A digital right management system according to claim 23, wherein said secure component detects whether any of said one or more self-protecting documents is tampered with.

29. A digital right management system according to claim 15, further comprising an encryption engine.

30. A digital right management system according to claim 15, further comprising a user-interface module.

31. A digital right management system according to claim 30, wherein said user-interface module includes one or more menus or toolbars.

32. A digital right management system according to claim 15, wherein said secure component acts as a shell to be compatible to plug-ins which are designed based on a predetermined specification of said secure component's interface.

33. A digital right management system according to claim 15, further comprising a software development kit that enables the creation of applications to protect, distribute, and consume content.

34. A digital right management system according to claim 15, wherein said system is connected to one or more storefronts.

35. A digital right management system according to claim 15, wherein said system is connected to one or more backoffices.

36. A digital right management system according to claim 15, wherein said system creates one or more rights labels.

37. A digital right management system according to claim 15, wherein said system creates one or more rights templates.

38. A digital right management system according to claim 15, wherein said system creates one or more metadata.

39. A digital right management system according to claim 15, wherein said secure component comprises a secure environment;

said interface comprises an application programming interface which provides interface between said secure environment and said software application;

said secure environment processes the requests coming from said software application through said application programming interface; and

said secure environment validates one or more documents.

40. A digital right management system according to claim 15, wherein said secure component comprises a secure environment;

said interface comprises an application programming interface which provides interface between said secure environment and said software application;

said secure environment processes the requests coming from said software application through said application programming interface; and

said secure environment validates one or more documents to verify that said one or more documents are compatible with said secure environment.

41. A digital right management system according to claim 15, wherein said secure component comprises a secure environment;

said interface comprises an application programming interface which provides interface between said secure environment and said software application;

said secure environment processes the requests coming from said software application through said application programming interface; and

said secure environment validates signatures of one or more documents to verify that said one or more documents are compatible with said secure environment.

42. A digital right management system according to claim 15, wherein said secure component comprises a secure container;

said interface comprises an application programming interface which provides interface between said secure container and said software application;

said secure container processes the requests coming from said software application through said application programming interface; and

said secure container validates signatures of one or more documents to verify that said one or more documents are compatible with said secure container.

43. A digital right management system according to claim 15, wherein said secure component comprises a secure repository;

said interface comprises an external interface which provides interface between a processing means and an external environment;

said secure repository processes requests for access to a digital work; and

said secure repository checks usage rights, and after checking, grants the access to said digital work.

44. A digital right management system according to claim 15, wherein said secure component comprises one of a secure container, a secure environment, and a secure repository.

45. A digital right management system according to claim 15, wherein said interface comprises an application programming interface.

46. A digital right management system according to claim 15, wherein in the case of verification of compatibility, said secure component initiates loading of one or more dynamically linked libraries.

47. A digital right management system according to claim 15, wherein in the case of incompatibility, said secure component refuses to load any data coming through said application programming interface.

X. EVIDENCE APPENDIX

There is no additional evidence relied upon in this brief.

XI. RELATED PROCEEDINGS APPENDIX

There are no related appeals or interferences.